

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-153956

(43) 公開日 平成10年(1998) 6月9日

(51) Int.Cl.<sup>6</sup>

G 0 9 C 1/00

識別記号

6 4 0

F I

G 0 9 C 1/00

6 4 0 B

6 4 0 D

6 4 0 Z

6 2 0 A

6 2 0 Z

6 2 0

審査請求 未請求 請求項の数11 O L (全 18 頁)

(21) 出願番号 特願平9-261762

(22) 出願日 平成9年(1997) 9月26日

(31) 優先権主張番号 特願平8-256945

(32) 優先日 平8(1996) 9月27日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 新保 淳

東京都府中市東芝町1番地 株式会社東芝

府中工場内

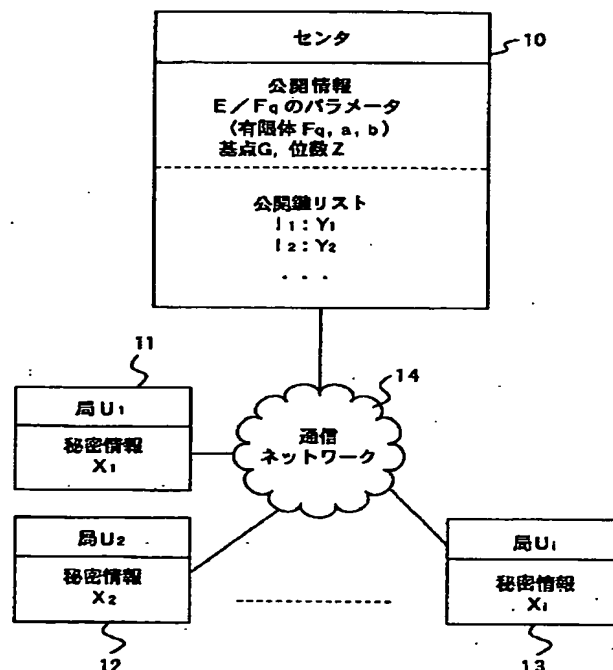
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 電子署名方法、電子署名システム及び、記録媒体

(57) 【要約】

【課題】 様々な運用形態を考慮した多重署名システムを容易に構成できる電子署名方法を提供する。

【解決手段】 有限体  $F_q$  上の楕円曲線  $E/F_q$  と、その上の基点  $G$  とを含むシステム情報と、楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y$  と、公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを用いて、任意に生成された乱数  $k$  と楕円曲線  $E/F_q$  上の基点  $G$  とに依存する点  $R$  の少なくとも一部のデータと、文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成し、文書データ  $M$  のみに依存する整数  $m$  と、点  $R$  に依存する整数  $r$  と、署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、システム情報と、署名者の公開鍵  $Y$  が与えられたときに、 $\pm s \cdot G = \pm m \cdot Y \pm r \cdot R$  over  $E/F_q$  で定義される関係式を用いて署名検査を行なう工程を具備する。



1

## 【特許請求の範囲】

【請求項 1】 文書データ M に対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、

有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y$  と、この公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを用いて、

任意に生成された乱数  $k$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成する署名データ生成工程と、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、前記署名者の公開鍵  $Y$  が与えられたときに、

$$\pm s \cdot G = \pm m \cdot Y \pm r \cdot R \text{ over } E/F_q$$

(+、- の符号は所定の条件により決定) で定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項 2】 文書データ  $M$  に対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、

有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y$  と、この公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを用いて、

任意に生成された乱数  $k$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成する署名データ生成工程と、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、前記署名者の公開鍵  $Y$  が与えられたときに、

前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と前記公開鍵  $Y$  との積からなる第 2 の項  $m \cdot Y$  と、前記整数  $r$  と前記楕円曲線  $E/F_q$  上の点  $R$  との積からなる第 3 の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

2

【請求項 3】  $n$  者から構成される複数の署名者の間で文書データ  $M$  に対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、

第  $i$  番目 ( $i = 1, 2, 3, \dots, n$ ) の署名者について、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y_i$  と、この公開鍵  $Y_i = x_i \cdot G$  を満たすように作成された署名者の秘密鍵  $x_i$  とを用いて、

複数の署名者の各々に対して生成された各乱数  $k_i$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と複数の署名者の各々に対する秘密鍵  $x_i$  と各乱数  $k_i$  とに依存する整数  $s$  とを含む署名データを生成する署名データ生成工程と、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、各公開鍵  $Y_i$  が与えられたときに、

$$\pm s \cdot G = \pm m \cdot (Y_1 + Y_2 + \dots + Y_n) \pm r \cdot R \text{ over } E/F_q$$

(+、- の符号は所定の条件により決定) で定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項 4】  $n$  者から構成される複数の署名者の間で文書データ  $M$  に対する電子署名データを作成し、この電子署名データに基づいて複数の署名者の署名検査を行なう電子署名方法であって、

第  $i$  番目 ( $i = 1, 2, 3, \dots, n$ ) の署名者について、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y_i$  と、この公開鍵  $Y_i = x_i \cdot G$  を満たすように作成された署名者の秘密鍵  $x_i$  とを用いて、

複数の署名者の各々に対して生成された各乱数  $k_i$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と複数の署名者の各々に対する秘密鍵  $x_i$  と各乱数  $k_i$  とに依存する整数  $s$  とを含む署名データを生成する署名データ生成工程と、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、各公開鍵  $Y_i$  が与えられたときに、

前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と各公開鍵  $Y_i$

3

( $i = 1, 2, 3, \dots, n$ ) の和との積からなる第 2 の項  $m \cdot (Y_1 + Y_2 + \dots + Y_n)$  と、前記整数  $r$  と前記楕円曲線  $E/F_q$  上の点  $R$  との積からなる第 3 の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項 5】  $n$  者から構成される複数の署名者の間で文書データ  $M$  に対する電子署名データを作成し、この電子署名データに基づいて複数の署名者の署名検査を行なう電子署名方法であって、

第  $i$  番目 ( $i = 1, 2, 3, \dots, n$ ) の署名者について、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y_i$  と、この公開鍵  $Y_i = x_i \cdot G$  を満たすように作成された署名者の秘密鍵  $x_i$  とを用いて、

複数の署名者の各々に対して生成された各乱数  $k_i$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の各点  $R_i$  の少なくとも一部のデータと、前記文書データ  $M$  と複数の署名者の各々に対する秘密鍵  $x_i$  と各乱数  $k_i$  とに依存する整数  $s$  とを含む署名データを生成する署名データ生成工程と、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の各点  $R_i$  及び前記文書データ  $M$  のうち少なくとも点  $R_i$  に依存する各整数  $r_i$  と、前記署名データである各点  $R_i$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、各公開鍵  $Y_i$  が与えられたときに、

前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と各公開鍵  $Y_i$

( $i = 1, 2, 3, \dots, n$ ) の和との積からなる第 2 の項  $m \cdot (Y_1 + Y_2 + \dots + Y_n)$  と、前記整数  $r_i$  と前記楕円曲線  $E/F_q$  上の各点  $R_i$  との積の和からなる第 3 の項  $(r_1 R_1 + r_2 R_2 + \dots + r_n R_n)$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程と、を具備することを特徴とする電子署名方法。

【請求項 6】 文書データ  $M$  に対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて署名検査を行なう署名検査装置とから構成される電子署名システムであって、

前記署名データ作成装置は、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y$  と、この公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを用いて、

任意に生成された乱数  $k$  と前記楕円曲線  $E/F_q$  上の基

4

点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成する手段を含み、

前記署名検査装置は、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、前記署名者の公開鍵  $Y$  が与えられたときに、前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と前記公開鍵  $Y$  との積からなる第 2 の項  $m \cdot Y$  と、前記整数  $r$  と前記楕円曲線  $E/F_q$  上の点  $R$  との積からなる第 3 の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含むことを特徴とする電子署名システム。

【請求項 7】  $n$  者から構成される複数の署名者の間で文書データ  $M$  に対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて複数の署名者の署名検査を行なう署名検査装置とから構成される電子署名システムであって、

前記署名データ作成装置は、

第  $i$  番目 ( $i = 1, 2, 3, \dots, n$ ) の署名者について、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y_i$  と、この公開鍵  $Y_i = x_i \cdot G$  を満たすように作成された署名者の秘密鍵  $x_i$  とを用いて、

複数の署名者の各々に対して生成された各乱数  $k_i$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と複数の署名者の各々に対する秘密鍵  $x_i$  と各乱数  $k_i$  とに依存する整数  $s$  とを含む署名データを生成する手段を含み、

前記署名検査装置は、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、各公開鍵  $Y_i$  が与えられたときに、

前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と各公開鍵  $Y_i$

( $i = 1, 2, 3, \dots, n$ ) の和との積からなる第 2 の項  $m \cdot (Y_1 + Y_2 + \dots + Y_n)$  と、前記整数  $r$  と前記楕円曲線  $E/F_q$  上の点  $R$  との積からなる第 3 の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含むことを特徴とする電子署名シス

10

20

30

40

50

テム。

【請求項 8】  $n$  者から構成される複数の署名者の間で文書データ  $M$  に対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて複数の署名者の署名検査を行なう署名検査装置とから構成される電子署名システムであって、

前記署名データ作成装置は、

第  $i$  番目 ( $i = 1, 2, 3, \dots, n$ ) の署名者について、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y_i$  と、この公開鍵  $Y_i = x_i \cdot G$  を満たすように作成された署名者の秘密鍵  $x_i$  とを用いて、

複数の署名者の各々に対して生成された各乱数  $k_i$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の各点  $R_i$  の少なくとも一部のデータと、前記文書データ  $M$  と複数の署名者の各々に対する秘密鍵  $x_i$  と各乱数  $k_i$  とに依存する整数  $s$  とを含む署名データを生成する手段を含み、

前記署名検査装置は、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の各点  $R_i$  及び前記文書データ  $M$  のうち少なくとも点  $R_i$  に依存する各整数  $r_i$  と、前記署名データである各点  $R_i$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、各公開鍵  $Y_i$  が与えられたときに、

前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と各公開鍵  $Y_i$

( $i = 1, 2, 3, \dots, n$ ) の和との積からなる第 2 の項  $m \cdot (Y_1 + Y_2 + \dots + Y_n)$  と、前記整数  $r_i$  と前記楕円曲線  $E/F_q$  上の各点  $R_i$  との積の和からなる第 3 の項 ( $r_1 R_1 + r_2 R_2 + \dots + r_n R_n$ ) との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含むことを特徴とする電子署名システム。

【請求項 9】 文書データ  $M$  に対する電子署名データを作成する処理と、作成された電子署名データに基づいて署名検査を行なう処理とをコンピュータに実行させる命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、

前記電子署名データを作成する処理は、

有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y$  と、この公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを用いて、

任意に生成された乱数  $k$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成し、

前記署名検査を行なう処理は、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、前記署名者の公開鍵  $Y$  が与えられたときに、前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と前記公開鍵  $Y$  との積からなる第 2 の項  $m \cdot Y$  と、前記整数  $r$  と前記楕円曲線  $E/F_q$  上の点  $R$  との積からなる第 3 の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう、ことを特徴とする記録媒体。

【請求項 10】  $n$  者から構成される複数の署名者の間で文書データ  $M$  に対する電子署名データを作成する処理と、作成された電子署名データに基づいて複数の署名者の署名検査を行なう処理とをコンピュータに実行させる命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、

前記電子署名データを作成する処理は、

第  $i$  番目 ( $i = 1, 2, 3, \dots, n$ ) の署名者について、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y_i$  と、この公開鍵  $Y_i = x_i \cdot G$  を満たすように作成された署名者の秘密鍵  $x_i$  とを用いて、

複数の署名者の各々に対して生成された各乱数  $k_i$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と複数の署名者の各々に対する秘密鍵  $x_i$  と各乱数  $k_i$  とに依存する整数  $s$  とを含む署名データを生成し、

前記署名検査を行なう処理は、

前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、各公開鍵  $Y_i$  が与えられたときに、

前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と各公開鍵  $Y_i$

( $i = 1, 2, 3, \dots, n$ ) の和との積からなる第 2 の項  $m \cdot (Y_1 + Y_2 + \dots + Y_n)$  と、前記整数  $r$  と前記楕円曲線  $E/F_q$  上の点  $R$  との積からなる第 3 の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう、ことを特徴とする記録媒体。

【請求項 11】  $n$  者から構成される複数の署名者の間で文書データ  $M$  に対する電子署名データを作成する処理と、作成された電子署名データに基づいて複数の署名者の署名検査を行なう処理とをコンピュータに実行させる

命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、  
前記電子署名データを作成する処理は、  
第  $i$  番目 ( $i = 1, 2, 3, \dots, n$ ) の署名者について、有限体  $F_q$  上の楕円曲線  $E/F_q$  と、この楕円曲線  $E/F_q$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/F_q$  上の点で定義される署名者の公開鍵  $Y_i$  と、この公開鍵  $Y_i = x_i \cdot G$  を満たすように作成された署名者の秘密鍵  $x_i$  とを用いて、  
複数の署名者の各々に対して生成された各乱数  $k_i$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の各点  $R_i$  の少なくとも一部のデータと、前記文書データ  $M$  と複数の署名者の各々に対する秘密鍵  $x_i$  と各乱数  $k_i$  とに依存する整数  $s$  とを含む署名データを生成し、  
前記署名検査を行なう処理は、  
前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の各点  $R_i$  及び前記文書データ  $M$  のうち少なくとも点  $R_i$  に依存する各整数  $r_i$  と、前記署名データである各点  $R_i$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、各公開鍵  $Y_i$  が与えられたときに、  
前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第 1 の項  $s \cdot G$  と、前記整数  $m$  と各公開鍵  $Y_i$  ( $i = 1, 2, 3, \dots, n$ ) の和との積からなる第 2 の項  $m \cdot (Y_1 + Y_2 + \dots + Y_n)$  と、前記整数  $r_i$  と前記楕円曲線  $E/F_q$  上の各点  $R_i$  との積の和からなる第 3 の項  $(r_1 R_1 + r_2 R_2 + \dots + r_n R_n)$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう、ことを特徴とする記録媒体。

\*

$$y^2 = x^3 + ax + b \quad (\text{但し } a, b, x, y \text{ は有限体 } F_q \text{ の元})$$

(1)

ここで、 $y^2$  は  $y$  の 2 乗を表し、 $x^3$  は  $x$  の 3 乗を表すものとする。以下、 $x^a$  で  $x$  の  $a$  乗を表す。

【0006】楕円曲線  $E/F_q$  の元は式 (1) を満たす  $(x, y)$  のペア (これを楕円曲線上の点と呼ぶ) と、無限遠点  $O$  とから成る。無限遠点  $O$  は有限体  $F_q$  の元のペア  $(x, y)$  という形式では表現できないが、実装上は無遠点を表す 1 ビットのフラグを用意すれば良い。この楕円曲線上の点の集合は加算に関して群を構成することが知られている。この加算に関して無限遠点  $O$  は単位元になる。

【0007】楕円曲線  $E/F_q$  のより詳細な説明や加算の定義などは例えば Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag にある。以下では特に断らない限り大文字で楕円曲線上の点 (すなわち、有限体  $F_q$  の元のペアもしくは無限遠点) を表し、小文字では有限体  $F_q$  の元もしくは自然数を表すこととする。なお、有限体  $F_q$  は  $q = p^t$  (但し  $p$  は素

## \* 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、電子的な文書に対する署名、捺印機能を実現する電子署名方法及び、この電子署名方法を用いて構成した電子署名システム、さらに、前記電子署名方法に関するプログラムが格納された記録媒体に関する。

## 【0002】

【従来の技術】電子署名 (デジタル署名) の作成法として様々な方式が考案されている。この中で代表的なものは素因数分解問題の困難性に基づく方式と離散対数問題の困難性に基づく方式である。このうち離散対数問題に基づく方式は、一般的な有限体上の乗法群を利用する方式と楕円曲線上の加法群を利用する方式が存在する。楕円曲線上の加法群における離散対数問題は有限体上の乗法群における離散対数問題や素因数分解問題に比べ、効率的な解法が発見されておらず、より安全性が高いといわれている。

【0003】従って、同じ安全性を確保してデジタル署名や公開鍵暗号方式を構成する場合、楕円曲線上の離散対数問題をベースに構築したシステムは他の問題をベースにした場合と比べてパラメータのサイズを小さく設定することが可能であり、このことが処理量の削減にもつながるという効果があることが知られている。

【0004】有限体  $F_q$  上の楕円曲線  $E/F_q$  は、有限体  $F_q$  の標数が 2 もしくは 3 以外の場合、次式 (1) 中のパラメータ  $a, b$  と有限体  $F_q$  で定義される。楕円曲線  $E/F_q$  は標数が 2 もしくは 3 の場合にも定義可能であるがここでは省略する。

## 【0005】

数、 $t$  は正整数) 個の元から成り、例えば、素体  $Z_p$  (0 から  $p-1$  までの整数で構成される) や 2 の拡大体  $GF(2^t)$  が典型的である。

【0008】楕円曲線上のデジタル署名方式の代表的な方式に楕円曲線上の ElGamal 署名がある。この方式では、公開鍵として楕円曲線を定義する有限体  $F_q$ 、 $a$ 、 $b$ 、基点  $G$ 、基点  $G$  の位数  $z$  を用いる。但し、基点  $G$  の位数  $z$  とは、 $z \cdot G = O$  over  $E/F_q$  を満たす最小の正整数を表す。

【0009】署名作成者の秘密鍵は位数  $z$  と互いに素で  $z$  未満の整数  $x$  であり、署名作成者の公開鍵は以下の点  $Y$  である。

$$Y = x \cdot G \text{ over } E/F_q$$

文書データ  $M$  のみに依存する整数  $m$  (これは一般にデジタルビット列で表現した文書データ  $M$  を暗号的なハッシュ関数により計算したダイジェスト情報である) に対するデジタル署名は以下の手順により作成される。ま

9

ず、位数  $z$  と互いに素で  $z$  未満の自然数である乱数  $k$  を決定し、この  $k$  から次式の  $R$  を求める。

$$【0010】 R = k \cdot G \text{ over } E/Fq$$

次に、楕円曲線上の点データを  $Z_z$  ( $z-1$  以下の自然数) の中へ変換する関数  $f$  を用いて、以下の  $r$  を求める。例えば、ハッシュ関数を用いれば良い。

$$【0011】 r = f(R)$$

さらに、以下の  $s$  を求める。

$$s = (m - x \cdot r) / k \pmod{z}$$

署名データは  $(R, s)$  のペアである。署名の検査は、 $m, R, s$  が次式を満たすことを検査することによって行われる。

$$【0012】 r = f(R)$$

$$m \cdot G = r \cdot Y + s \cdot R \text{ over } E/Fq$$

ElGamal 署名方式(ElGamal signature scheme) は、“T.ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. IT, Vol.IT-31, No.4, July 1985, pp.469-472” に詳細に記載されている。

【0013】 以上の電子署名方式により一般の電子文書に対する捺印機能を実現することができるが、さらに、電子的な回覧文書に対する複数の署名者(signer)による捺印機能も要望される。このような機能は複数の署名者による同一の文書に対する署名データを連結することで構成できる。しかし、このような構成では署名者数に比例して署名データ量と署名検査の処理量が増加する欠点がある。単純に個別の署名を連結する場合に比べて、署名データサイズの増加が少なく抑えられる方式、あるいは、署名検査の処理量が抑えられる方式が考案されており、これらは多重署名法と呼ばれている。

#### 【0014】

【発明が解決しようとする課題】 しかしながら、上記した多重署名法は、楕円曲線上の離散対数問題の困難性に基づくElGamal 署名方式を用いたものではなかった。本発明はこのような課題に着目してなされたものであり、その目的とするところは、様々な運用形態を考慮した多重署名システムを容易に構成できる楕円曲線を利用した電子署名方法、及びこの電子署名方法を用いて構成した電子署名システム、さらには前記電子署名方法に関するプログラムが格納された記録媒体を提供することにある。

#### 【0015】

【課題を解決するための手段】 上記の目的を達成するために、本発明の電子署名方法は、文書データMに対する電子署名データを作成し、この電子署名データに基づいて署名検査を行なう電子署名方法であって、有限体  $Fq$  上の楕円曲線  $E/Fq$  と、この楕円曲線  $E/Fq$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/Fq$  上の点で定義される署名者の公開鍵  $Y$  と、この公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを

10

用いて、任意に生成された乱数  $k$  と前記楕円曲線  $E/Fq$  上の基点  $G$  とに依存する楕円曲線  $E/Fq$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成する署名データ生成工程と、前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/Fq$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、前記署名者の公開鍵  $Y$  が与えられたときに、 $\pm s \cdot G = \pm m \cdot Y \pm r \cdot R \text{ over } E/Fq$  (+、- の符号は所定の条件により決定) で定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう署名検査工程とを具備する。

【0016】 また、本発明の電子署名システムは、文書データ  $M$  に対する電子署名データを作成する署名データ作成装置と、前記電子署名データに基づいて署名検査を行なう署名検査装置とから構成される電子署名システムであって、前記署名データ作成装置は、有限体  $Fq$  上の楕円曲線  $E/Fq$  と、この楕円曲線  $E/Fq$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/Fq$  上の点で定義される署名者の公開鍵  $Y$  と、この公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを用いて、任意に生成された乱数  $k$  と前記楕円曲線  $E/Fq$  上の基点  $G$  とに依存する楕円曲線  $E/Fq$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成する手段を含み、前記署名検査装置は、前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/Fq$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、前記署名者の公開鍵  $Y$  が与えられたときに、前記整数  $s$  と前記楕円曲線  $E/Fq$  上の基点  $G$  との積からなる第1の項  $s \cdot G$  と、前記整数  $m$  と前記公開鍵  $Y$  との積からなる第2の項  $m \cdot Y$  と、前記整数  $r$  と前記楕円曲線  $E/Fq$  上の点  $R$  との積からなる第3の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう手段を含む。

【0017】 また、本発明の記録媒体は、文書データ  $M$  に対する電子署名データを作成する処理と、作成された電子署名データに基づいて署名検査を行なう処理とをコンピュータに実行させる命令を含むプログラムを格納した、コンピュータが読み取り可能な記録媒体であって、前記電子署名データを作成する処理は、有限体  $Fq$  上の楕円曲線  $E/Fq$  と、この楕円曲線  $E/Fq$  上の基点  $G$  とを含むシステム情報と、前記楕円曲線  $E/Fq$  上の点で定義される署名者の公開鍵  $Y$  と、この公開鍵  $Y = x \cdot G$  を満たすように作成された署名者の秘密鍵  $x$  とを用い

11

て、任意に生成された乱数  $k$  と前記楕円曲線  $E/F_q$  上の基点  $G$  とに依存する楕円曲線  $E/F_q$  上の点  $R$  の少なくとも一部のデータと、前記文書データ  $M$  と秘密鍵  $x$  と乱数  $k$  とに依存する整数  $s$  とを含む署名データを生成し、前記署名検査を行なう処理は、前記文書データ  $M$  のみに依存する整数  $m$  と、前記楕円曲線  $E/F_q$  上の点  $R$  及び前記文書データ  $M$  のうち少なくとも点  $R$  に依存する整数  $r$  と、前記署名データである点  $R$  の少なくとも一部のデータ及び整数  $s$  と、前記システム情報と、前記署名者の公開鍵  $Y$  が与えられたときに、前記整数  $s$  と前記楕円曲線  $E/F_q$  上の基点  $G$  との積からなる第1の項  $s \cdot G$  と、前記整数  $m$  と前記公開鍵  $Y$  との積からなる第2の項  $m \cdot Y$  と、前記整数  $r$  と前記楕円曲線  $E/F_q$  上の点  $R$  との積からなる第3の項  $r \cdot R$  との間の特定の演算により定義される関係式またはこの関係式と等価な関係式を署名検査式として用いて署名検査を行なう。

【0018】

【発明の実施の形態】まず、本実施形態の概略を説明する。第1の概略に係る電子署名方式は、楕円曲線上のElGamal署名方式を変形した電子署名方式であり、従来の楕円曲線上のElGamal署名方式との相違点は、署名検査式における文書データ  $M$  と、署名データ  $s$  と、乱数から生成された署名データ  $R$  及び文書データ  $M$  のうち少なくとも署名データ  $R$  に依存する整数  $r$  の各々を互いに所定の規則に基づいて置き換えたことにある。各署名者の秘密鍵が作用した  $s$  が  $s = m \cdot x + r \cdot k \pmod{z}$  という形式で作成されるので、秘密鍵  $x$  が複数になっても、多重署名の場合は文書データ  $M$  が共通なので、複数の秘密鍵  $x$  が加算によりまとめられる。このことにより、同方式の多重署名方式への拡張が容易になるという利点が得られる。

【0019】なお、 $r \cdot k$  は秘密鍵  $x$  が複数になっても影響を受けない項であるから、整数  $r$  は乱数から生成された点  $R$  のみに依存させる構成以外に、点  $R$  と文書データ  $M$  の両方に依存させる構成でもよく、その方が安全性の向上が期待できる。

【0020】このように楕円曲線上のElGamal署名方式を変形しても公開鍵  $Y$  に対応する秘密鍵  $x$  を保持する署名者は検査式を満たす署名データ  $R, s$  を作成できる。一方、秘密鍵  $x$  を保持しない場合に署名データ  $R, s$  を求めるには、楕円曲線上の離散対数問題を求める以外の方法は考案されていない。従って、電子署名方式として有効である。

【0021】次に第2の概略を説明する。第2の概略では、第1の概略における電子署名方式を多重署名方式として適用する。複数の署名者がそれぞれ乱数  $k$  を作成し、各々の乱数  $k$  に依存した楕円曲線上の点  $R$  を最初にデータを一巡させることで作成する。その後、各々の署名者が自身の作成した乱数  $k$  と秘密鍵  $x$  から部分署名  $s$  を作成し、これを巡回する。

12

【0022】部分署名  $s$  の巡回においては、それ以前の署名者による部分署名に各自の部分署名を融合させる。こうして最後の署名者の処理により多重署名データ  $R, s$  が作成される。

【0023】署名検査における検査式は第1の概略における検査式の公開鍵  $Y$  を複数の署名作成者の個々の公開鍵  $Y_i$  の和に置き換えたものである。秘密鍵  $x_i$  が一つでも関与しない場合には、検査式を満たす  $R, s$  は得られない。従って、複数の署名者による電子署名方式として有効である。

【0024】次に第3の概略を説明する。第3の概略では、第1の概略における電子署名方式を逐次型（一巡型）の多重署名方式に適用する。複数の署名者がそれぞれ乱数  $k$  を作成し、この乱数  $k$  に依存した楕円曲線上の点  $R$  を作成する。各署名者は、前の署名者から得た部分署名  $s$  に自分の秘密鍵  $x$  と点  $R$  の生成に利用した乱数  $k$  を融合させて、新たな部分署名  $s$  を作成し、これを次の署名者に送る。この部分署名  $s$  と同時に、独立に生成した点を署名データの一部として追加していく。こうして最後の署名者の処理により多重署名データ  $s, R_1, R_2, \dots, R_n$  が作成される。

【0025】署名検査における検査式は第1の概略における検査式の公開鍵  $Y$  を複数の署名作成者の個々の公開鍵  $Y_i$  の和に置き換え、さらに点  $R$  の項を個々の署名者による  $r_i \cdot R_i$  の和に置き換えたものを用いる。

【0026】以下に、図面を参照して上記した概略を詳細に説明する。図1は本発明の第1実施形態に係る電子署名システムの基本構成を示す図である。図1に示すように、本システムはセンタ10と利用者に対応する複数の局(entities)11、12、13 ( $U_1, U_2, \dots, U_i$ ) から成る通信ネットワーク14により構成される。センタ10は公開情報として、楕円曲線  $E/F_q$  のパラメータを生成して公開する。また、楕円曲線  $E/F_q$  上の基点  $G$  とその位数  $z$  を求めて公開する。

【0027】さらに、関数  $f$  と関数  $h$  を公開する。これらは暗号的なハッシュ関数であり、任意のサイズの入力に対し、そのダイジェスト情報として160bit程度の固定長の整数を出力する。具体例は、SHAやMD5、RIPE-MDなどである。また、関数  $f$  と  $h$  は共通でも良い。

【0028】各局  $U_i$  は  $z-1$  以下の自然数である乱数  $x_i$  を定め、この  $x_i$  を局秘密鍵とする。さらに、局公開鍵  $Y_i$  を次式により定める。

$$Y_i = x_i \cdot G \text{ over } E/F_q$$

局  $U_i$  は局公開鍵  $Y_i$  をセンタ10に送り、センタ10は公開鍵リストの局  $U_i$  のエリアに  $Y_i$  を登録する。公開鍵リストの書き換えはセンタ10のみが実行でき、同リストの読み出しは任意の局が実行できる。なお、局  $U_i$  のID情報（識別情報）を  $I_i$  とする。

【0029】図2Aは、局  $U_i$  が文書データ  $M$  に対する

10

20

30

40

50

デジタル署名を作成する手順である。

<局  $U_i$  の手順>

- 1: 乱数  $k$  ( $1 < k < z-1$ ) を定める。… (ステップ 101)
- 2:  $R = k \cdot G$  over  $E/Fq$  を計算する。… (ステップ 102)
- 3:  $r = f(R)$  を計算する。… (ステップ 103)
- 4:  $m = h(M)$  を計算する。… (ステップ 104)
- 5:  $m$ ,  $r$  と秘密鍵  $x_i$  から  $s = x_i \cdot m + k \cdot r \bmod z$  を計算する。

【0030】… (ステップ 105)

以上により作成された  $R$  と  $s$  が局  $U_i$  の文書データ  $M$  に対するデジタル署名となる。

【0031】この署名作成手続きにおけるステップ 101 から 103 は、文書データ  $M$  に依存しないため、デジタル署名作成の要求が生じる前に計算し、 $(k, R, r)$  を幾つか蓄積しておくことができる。このようにすると、署名作成要求時の処理はステップ 104, 105 のみとなり、処理時間面で有効である。

【0032】次に図 2B を参照しながら、本デジタル署名の検査手順を説明する。

<署名検査手順>

- 1: 公開リストから局  $U_i$  の公開鍵  $Y_i$  を取り出す。

【0033】… (ステップ 106)

- 2:  $r = f(R)$  を計算する。… (ステップ 107)
- 3:  $m = h(M)$  を計算する。… (ステップ 108)
- 4:  $r$ ,  $s$ ,  $m$ ,  $Y_i$  が次式の関係を満たすことを確認 \*

$$(s/r) \cdot G - (m/r) \cdot Y_i = R \text{ over } E/Fq, \quad \dots (2)$$

$$(s/m) \cdot G - (r/m) \cdot R = Y_i \text{ over } E/Fq,$$

$$(m/s) \cdot Y_i + (r/s) \cdot R = G \text{ over } E/Fq$$

などを検査することと等価であることは、検査式における左辺もしくは右辺の項の移項と  $s$ ,  $m$ ,  $r$  の  $Fq$  における逆数を両辺に掛けることから明らかである。

【0038】また、検査式における  $s \cdot G$ ,  $m \cdot Y_i$ ,  $r \cdot R$  の 3 項の符号を変えること (すなわち、+ を - にしたり、その逆、具体的には  $\pm s \cdot G = \pm m \cdot Y_i \pm r \cdot R = O$  over  $E/Fq$  でもよく、+、- の符号は以下の説明の通り、署名生成過程におけるステップにより決定される) も署名生成課程におけるステップ 105 の  $s$ ,  $x_i \cdot m$ ,  $k \cdot r$  の符号を変えることに相当するため、検査式における 3 項の符号を変えた署名方式は本質的に本実施形態の方式と同値であることにも注意されたい。

【0039】なお、本発明の署名方式において、 $f(R)$  の代わりに  $f(R, M)$  を用いてもよい。 $f(R, M)$  は署名者がランダムに決定した、楕円曲線上の点  $R$  のデータと文書データ  $M$  の両方に依存したハッシュ値を表している。具体的には  $R$  と  $M$  とを連結してハッシュする、 $R$  のデータを鍵として鍵付きハッシュ (Keyed hash) 法を利用するなどである。

\*する。

【0034】… (ステップ 109)

$$s \cdot G = m \cdot Y_i + r \cdot R \text{ over } E/Fq$$

この関係が成立する場合には、 $(R, s)$  は局  $U_i$  の文書データ  $M$  に対するデジタル署名であるものと判定する。

【0035】ステップ 101 から 105 の手順により生成された  $(R, s)$  がステップ 109 の検査式を満足することは明らかである。逆に文書データ  $M$  が与えられた状態で、 $Y_i$  の離散対数  $x_i$  を持たない局がステップ 109 の検査式を満たす  $(R, s)$  の組を求めることは楕円曲線上の離散対数問題を求めることと同程度に困難であると考えられる。例えば、最初に  $R$  を定めると  $s \cdot G = \text{const over } E/Fq$  なる  $s$  を求めることになり、これは離散対数問題に他ならない。一方、 $s$  を先に定めると  $r \cdot R = \text{const over } E/Fq$  なる  $R$  を求めることになり、この解法も一般に知られていない。

【0036】なお、本実施形態のデジタル署名方法で用いられる署名検査式の変形には様々なものが考えられるが、以下に代表的なものを示す。これらは本質的に同じ検査を実行していることに注意されたい。

【0037】まず、ステップ 109 の検査式は、

$$s \cdot G - m \cdot Y_i - r \cdot R = O \text{ over } E/Fq,$$

$$-s \cdot G + m \cdot Y_i + r \cdot R = O \text{ over } E/Fq$$

などを検査することと等価であることは検査式における左辺もしくは右辺の項を移項することから明らかである。さらに、

【0040】変形手順ではステップ 103 とステップ 107 が  $r = f(R, M)$  に変更される。一般にはこのように変形した手順の方が、 $R$  と  $M$  から  $r$  が作成されたことが保証されるために安全性が向上する。

【0041】本実施形態の特徴は、署名者が署名作成毎に生成する乱数と基点  $G$  に依存した項  $r \cdot R$  と署名者の公開鍵  $Y_i$  と署名対象である文書データ  $M$  のみに依存した項  $m \cdot Y_i$  と署名者の秘密鍵  $x_i$  が作用した  $s$  により基点  $G$  を加算する回数を変化させた項  $s \cdot G$  の 3 つの項の加算が無窮遠点に一致するかどうかを判定することにある。

【0042】このうち式 (2) を検査式とする場合には、署名データサイズの削減が可能である。以下にその具体的な手順を示す。局  $U_i$  が文書データ  $M$  に対するデジタル署名を作成する手順は基本的に先の手順と同じであるが、ステップ 107 における  $r$  が位数  $z$  と互いに素であるかどうかを確認する。もし、互いに素でない場合には、ステップ 101 に戻り別の乱数  $k$  を生成する。最終的に出力されるデジタル署名のデータは  $r$  と  $s$  であり点  $R$  の代わりに  $r$  を用いる。このことにより署名デ



15

ータサイズが約 2/3 にできる。

【0043】次に上記した検査手順を変形したデジタル署名の検査手順を図3を参照して説明する。

<署名検査手順>

1: 公開リストから局  $U_i$  の公開鍵  $Y_i$  を取り出す。

【0044】… (ステップ1101)

2:  $m = h(M)$  を計算する。… (ステップ1102)

3:  $1/r \pmod{Z}$  を計算する。… (ステップ1103)

4: 次式の点  $R$  を計算する。… (ステップ1104)

$R = (s/r) \cdot G - (m/r) \cdot Y_i \text{ over } E/F_q$

5: 点  $R$  と署名データの  $r$  が次式の関係を満たすことを確認する。

【0045】… (ステップ1105)

$r = f(R)$

この関係が成立する場合には、 $(r, s)$  は局  $U_i$  の文書データ  $M$  に対するデジタル署名であるものと判定する。

【0046】次に、図1に示したデジタル署名を多重署名に適用した第2実施形態の電子署名方法を説明する。図4A、4Bは多重署名における情報の流れを表し、図5A、5Bは各局の処理手順を表す。

【0047】ここでは、局  $U_1, U_2, \dots, U_n$  の  $n$  局が文書データ  $M$  に多重署名する場合を想定する。多重署名の作成は図4Aの  $R_n$  の作成ラウンドと、図4Bの  $s_n$  の作成ラウンドの2回の巡回操作から成る。図5Aは  $R_n$  の作成ラウンドにおける局  $U_i$  の処理手順、図5Bは  $s_n$  の作成ラウンドにおける局  $U_i$  の処理手順をそれぞれ示す。

(1)  $R_n$  の作成ラウンド

<局  $U_i$  の手順> ( $i = 1, 2, \dots, n$ )

1: 乱数  $k_i$  ( $1 < k_i < z-1$ ) を作成する。… (ステップ301)

2: 局  $U_{(i-1)}$  から受信した情報  $R_{(i-1)}$  と乱数  $k_i$  から次式の  $R_i$  を作成する。

【0048】 $R_i = R_{(i-1)} + k_i \cdot G \text{ over } E/F_q$   
… (ステップ302)

3: 情報  $R_i$ 、文書データ  $M$  を局  $U_{(i+1)}$  に送信する。… (ステップ303)

以上の処理を局  $U_1$  から順番に局  $U_n$  まで実行し、 $R_n$  を作成する。なお、局  $U_1$  は、 $R_0 = O$  (無限遠点) としてステップ302の処理を行う。

【0049】また、局  $U_n$  は作成した情報  $R_n$  から  $r = f(R_n)$  により  $r$  を求め、これを局  $U_1$  に送信し、 $s_n$  の作成ラウンドに移る。

(2)  $s_n$  の作成ラウンド

<局  $U_i$  の手順> ( $i = 1, 2, \dots, n$ )

1: 局  $U_1, U_2, \dots, U_{(i-1)}$  の公開鍵  $Y_1, Y_2, \dots, Y_{(i-1)}$  を公開鍵リストから取り出す。… (ステップ304)

16

2: 局  $U_{(i-1)}$  から  $R_n$  の作成ラウンドで受信した  $R_{(i-1)}$  と、このラウンドで局  $U_{(i-1)}$  から受信した  $r, s_{(i-1)}$  が次の関係を満たしていることを確認する。… (ステップ305)

$m = h(M)$  を計算、

$s_{i-1} \cdot G = m \cdot (Y_1 + Y_2 + \dots + Y_{i-1}) + r \cdot R_{i-1} \text{ over } E/F_q$

3: ステップ305の関係を満足していない場合には、局  $U_{i-1}$  の処理に異常があったものとして処理を打ち切る。… (ステップ306)

4: 先のラウンドで作成した乱数  $k_i$  と自局の秘密鍵  $x_i$  を用いて次式の  $s_i$  を計算する。… (ステップ307)

$s_i = s_{i-1} + x_i \cdot m + k_i \cdot r \pmod{z}$

5:  $s_i, r$  を局  $U_{i+1}$  に送る。… (ステップ308)

以上の処理を局  $U_1$  から順番に局  $U_n$  まで実行し、 $s_n$  を作成する。なお、局  $U_1$  は、 $s_0 = 0$  としてステップ307の処理を行う。

【0050】以上により作成された  $(R_n, s_n)$  が局  $U_1$  から  $U_n$  による文書データ  $M$  に対する多重署名である。局  $U_n$  は作成した署名情報  $(R_n, s_n)$  を必要に応じて全ての局  $U_1, U_2, \dots, U_{n-1}$  に送る。

【0051】なお、上記手順のうちステップ304、305、306は部分署名  $s_{i-1}$  の検査を実行する部分であり、省略することも可能である。この部分署名の検査を省略した場合、多重署名  $(R_n, s_n)$  が作成された後になってはじめて検査を実行することになる。署名作成者の不正をできるだけ早期に検出するためにはステップ304、305、306の部分署名の検査が有効である。

【0052】図6は図5A、5Bの手順により作成された多重署名の検査手順を示す。検査時には以下の処理を行う。署名検査には  $R_n, s_n, M$  および局のID情報  $I_1, I_2, \dots, I_n$  が必要である。

【0053】1: 局  $U_1, U_2, \dots, U_n$  の公開鍵  $Y_1, Y_2, \dots, Y_n$  を公開鍵リストから取り出す。… (ステップ401)

2:  $R_n, s_n, M$  が次の関係を満たすことを確認する。… (ステップ402)

$m = h(M)$  を計算、

$r = f(R_n)$  を計算、

$s_n \cdot G = m \cdot (Y_1 + Y_2 + \dots + Y_n) + r \cdot R_n \text{ over } E/F_q$

この関係が成立する場合には、 $(R_n, s_n)$  は正当な多重署名であるものと判定する。

【0054】なお、以上に示した多重署名作成手順及び多重署名検査手順でも  $r = f(R_n)$  の代わりに  $r = f(R_n, M)$  に変更し、さらに多重署名検査手順におけるステップ402において  $r = f(R_n, M)$  に変更することもできる。

17

【0055】次に、図3に示した署名検査手順をこの多重署名に適用する手順を説明する。局 $U_i$ が文書データ $M$ に対するデジタル署名を作成する手順は基本的に図5A、5Bの手順と同じであるが、ここでは、局 $U_n$ におけるステップ302における計算の結果として生じる $R_n$ に対し $r = f(R_n)$ を計算し、 $r$ が位数 $z$ と互いに素かどうかを確認する。もし、互いに素でない場合には、ステップ301に戻り別の乱数 $k_n$ を生成する。 $R_n$ の生成ラウンドで局 $U_n$ が出力する $r$ は $z$ と互いに素である。また、2巡目が終了して最終的に出力される多重署名のデータは $r$ と $s_n$ である。

【0056】次にこのデジタル署名の検査手順を説明する。図7はこの手順により作成された多重署名の検査手順を示す。

1：局 $U_1, U_2, U_n$ の公開鍵 $Y_1, Y_2, \dots, Y_n$

を公開鍵リストから取り出す。…(ステップ1201)

2： $m = h(M)$ を計算…(ステップ1202)

3： $1/r \pmod{Z}$ を計算する。…(ステップ1203)

4：次式の点 $R_n$ を計算する。…(ステップ1204)

$R_n = (s_n / r) \cdot G - (m / r) \cdot (Y_1 + Y_2 + \dots + Y_n) \text{ over } E/Fq$

5：点 $R_n$ と署名データの $r$ が次式の間接関係を満たすことを確認する。…(ステップ1205)

$r = f(R_n)$

この関係が成立する場合には、 $(r, s_n)$ は正当な多重署名であるものと判定する。

【0057】次に、図2A、2Bに示したデジタル署名を多重署名に適用した第3実施形態の電子署名方法を説明する。第3実施形態における情報の流れを図8に示す。ここでは複数の署名作成局間で情報を1巡させるだけで多重署名データを生成する。局 $U_1, U_2, \dots, U_n$ の $n$ 局が多重署名を作成するものとする。図9は局 $U_i$ の手順を示す。

<局 $U_i$ の手順> ( $i = 1, 2, \dots, n$ )

1：局 $U_1, U_2, \dots, U_{i-1}$ の公開鍵 $Y_1, Y_2, \dots, Y_{i-1}$ を公開鍵リストから取り出す。…(ステップ601)

2：局 $U_{i-1}$ から受信した $R_1, R_2, \dots, R_{i-1}, s_{i-1}, M$ が次の関係を満たしていることを確認する。…(ステップ602)

$m = h(M)$ を計算、

$r_j = f(R_j) \ (j = 1, 2, \dots, i-1)$ を計算、  
 $s_{i-1} \cdot G = m \cdot (Y_1 + \dots + Y_{i-1}) + r_1 \cdot R_1 + r_2 \cdot R_2 + \dots + r_{i-1} \cdot R_{i-1} \text{ over } E/Fq$

3：ステップ602の関係を満足していない場合には、局 $U_{i-1}$ の処理に異常があったものとして処理を打ち切る。…(ステップ603)

4：乱数 $k_i \ (1 < k_i < z-1)$ を作成する。…(ステップ604)

18

5：乱数 $k_i$ から次式の $R_i$ を作成する。…(ステップ605)

$R_i = k_i \cdot G \text{ over } E/Fq$

6：局 $U_{i-1}$ から受信した情報 $s_{i-1}$ と乱数 $k_i$ 、自局の秘密鍵 $x_i$ から次式の $s_i$ を計算する。…(ステップ606)

$r_i = f(R_i)$ を計算、

$s_i = s_{i-1} + x_i \cdot m + k_i \cdot r_i \pmod{z}$

7：データ $s_i, R_1, R_2, \dots, R_i$ 、文書データ $M$ を局 $U_{i+1}$ に送信する。

【0058】…(ステップ607)

以上の処理を局 $U_1$ から順番に局 $U_n$ まで実行し、作成された $s_n, R_1, R_2, \dots, R_n$ が局 $U_1$ から $U_n$ による文書データ $M$ に対する多重署名である。なお、局 $U_1$ は、 $R_0 = O$  (無限遠点)、 $s_0 = 0$ としてステップ605、606の処理を行い、ステップ601から603までの部分署名の検査処理は行わない。

【0059】図9の手順により作成された多重署名の検査手順を図10を参照しながら説明する。

1：局 $U_1, U_2, U_n$ の公開鍵 $Y_1, Y_2, \dots, Y_n$

を公開鍵リストから取り出す。…(ステップ701)

2： $s_n, R_1, R_2, \dots, R_n, M$ が次の関係を満たすことを確認する。

【0060】…(ステップ702)

$m = h(M)$ を計算、

$r_j = f(R_j) \ (j = 1, 2, \dots, i-1)$ を計算、  
 $s_n \cdot G = m \cdot (Y_1 + \dots + Y_n) + r_1 \cdot R_1 + r_2 \cdot R_2 + \dots + r_n \cdot R_n \text{ over } E/Fq$

この関係が成立する場合には、 $(s_n, R_1, R_2, \dots, R_n)$ は正当な多重署名であるものと判定する。

【0061】なお、図9、図10に示した多重署名方法は、図5A、5B、図6の多重署名法に比べて、データ・サイズと検査時の処理量からは不利であるが、署名作成が1巡の処理で行えるという利点を持つ。

【0062】また、他の実施形態と同様に本多重署名手順でも $r = f(R_i)$ の代わりに $r = f(R_i, M)$ を利用してもよい。具体的には、局 $U_i$ の多重署名作成手順におけるステップ602にて $r_j = f(R_j, M)$

( $j = 1, 2, \dots, i-1$ )を計算し、ステップ606にて、 $r_i = f(R_i, M)$ を計算するようにそれぞれ変更する。

【0063】多重署名の検査手順では、ステップ702にて $r_j = f(R_j, M)$  ( $j = 1, 2, \dots, i-1$ )を計算するように変更する。図11は、本実施形態の電子署名方式の作成・検査を実行する装置の一構成を示す。

【0064】演算器901は多倍長の演算を実行する部分であり、本電子署名方式の演算処理の大部分を実行する。乱数発生器902は署名作成時に必要な乱数 $k$ を生成する部分である。乱数メモリ903は乱数発生器90

19

2で発生された乱数 $k$ と、乱数 $k$ から計算される $R = k \cdot G \text{ over } E/Fq$ の値と、 $r = f(R)$ の値のペアを蓄積する部分である。乱数発生器902、演算器901は署名作成時・検査時以外にも稼働し、乱数( $k$ ,  $R$ ,  $r$ )のペアを生成し、乱数メモリ903に蓄積する。秘密鍵メモリ904は局の秘密鍵を格納するメモリである。その他に制御部905、メモリ906、入出力部907から構成される。

【0065】最後に、本実施形態の署名方式の変形例の一つを示す。局 $U_i$ が文書データ $M$ に対するデジタル署名を作成する手順は以下の通りである。

<局 $U_i$ の手順>

- 1: 乱数 $k$  ( $1 < k < z-1$ ) を定める。… (ステップ1001)
- 2:  $R = k \cdot G \text{ over } E/Fq$  を計算する。… (ステップ1002)
- 3:  $r = f(R)$  を計算する。… (ステップ1003)
- 4:  $m = h(M, R)$  を計算する。… (ステップ1004)
- 5:  $m$ ,  $r$  と秘密鍵 $x_i$  から  $s = x_i \cdot m + k \cdot r \text{ mod } z$  を計算する。

【0066】… (ステップ1005)

以上により作成された $R$ と $s$ が局 $U_i$ の文書データ $M$ に対するデジタル署名となる。

【0067】本デジタル署名の検査手順は以下の通りである。

<署名検査手順>

- 1: 公開鍵リストから局 $U_i$ の公開鍵 $Y_i$ を取り出す。

【0068】

… (ステップ1006)

- 2:  $r = f(R)$  を計算する。… (ステップ1007)
- 3:  $m = h(M, R)$  を計算する。… (ステップ1008)
- 4:  $r$ ,  $s$ ,  $m$ ,  $Y_i$  が次式の関係を満たすことを確認する。… (ステップ1009)

$$s \cdot G = m \cdot Y_i + r \cdot R \text{ over } E/Fq$$

この関係が成立する場合には、( $R$ ,  $s$ )は局 $U_i$ の文書データ $M$ に対するデジタル署名であるものと判定する。

【0069】この方式では $m$ の計算において、文書データ $M$ のみでなくランダムに生成された点 $R$ のデータを作図させてハッシングしている。一般にはこのようにした方が安全性が向上するものと考えられる。なお、 $m = h(M, r)$ としても良い。

【0070】この変形方式における2巡型多重署名(図5A、5Bおよび図6)の手順は単純に $m = h(M, R)$ に置き換えれば良い。1巡型多重署名(図9および図10)の手順では、署名者により $m_1 = h(M, R_1)$ ,  $m_2 = h(M, R_2)$ , ...,  $m_n = h(M, R_n)$

20

$n$ )と異なる $m$ が生成されるので、検査式も $s_i \cdot G = m_1 \cdot Y_1 + \dots + m_n \cdot Y_n + r_1 \cdot R_1 + \dots + r_n \cdot R_n$ と変更される。

【0071】また、図12A、12Bに示すような手順の多重署名方法を用いた場合でも、図3、図7に示した検査手順を適用することができる。以上のように、本実施形態によれば、楕円曲線上のElGamal署名を变形し、2巡型や1巡型の多重署名を容易に構成可能な電子署名方法が提供できる。

【0072】なお、上記した各実施形態における、電子署名データを作成する処理及び作成された電子署名データに基づいて署名検査を行なう処理は、プログラムとしてコンピュータが読み取り可能な記録媒体に格納し、コンピュータに実行させることが可能である。

【0073】

【発明の効果】以上述べたように本発明によれば、様々な運用形態を考慮した多重署名システムを容易に構成できる電子署名方法、電子署名システム、及び記録媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係る電子署名システムの基本構成を示す図である。

【図2】(a)は、本発明の第1実施形態に係る電子署名方法において、署名作成手順を示す図であり、(b)は検査手順を示す図である。

【図3】本発明の第1実施形態に係る電子署名方法を变形した署名検査手順を示す図である。

【図4】本発明の第2実施形態に係る2巡型の多重署名方法における情報の流れを示す図である。

【図5】2巡型の多重署名方式の署名作成手順を示す図である。

【図6】2巡型の多重署名方式の検査手順を示す図である。

【図7】2巡型の多重署名方法を变形した署名検査手順を示す図である。

【図8】本発明の第3実施形態に係る1巡型の多重署名方法における情報の流れを示す図である。

【図9】1巡型の多重署名方法における署名作成手順を示す図である。

【図10】1巡型の多重署名方法の検査手順を示す図である。

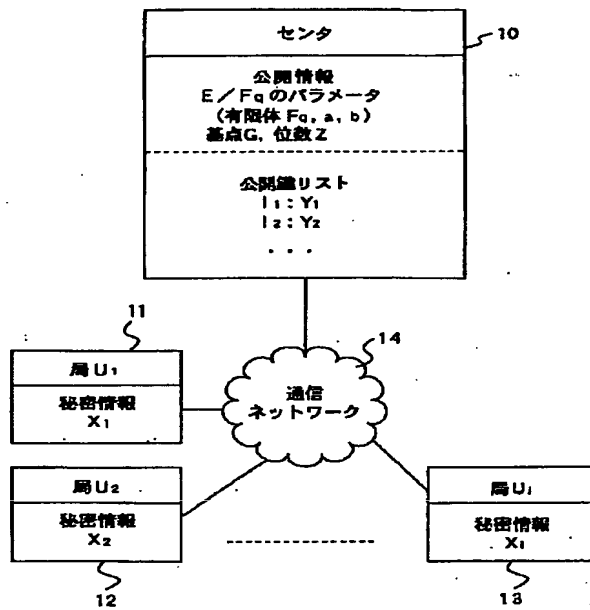
【図11】電子署名データの作成及び検査を行なう装置の構成例を示す図である。

【図12】署名手順の変形例を示す図である。

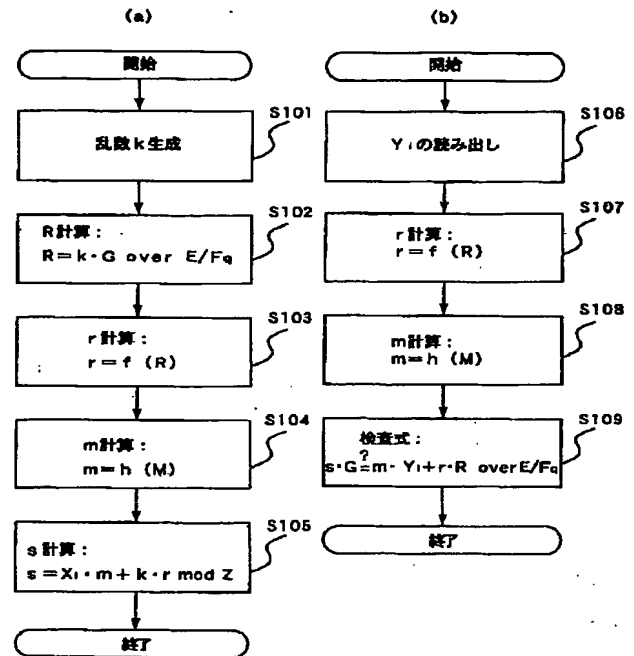
【符号の説明】

- 10…センタ、
- 11、12、13…局、
- 14…通信ネットワーク。

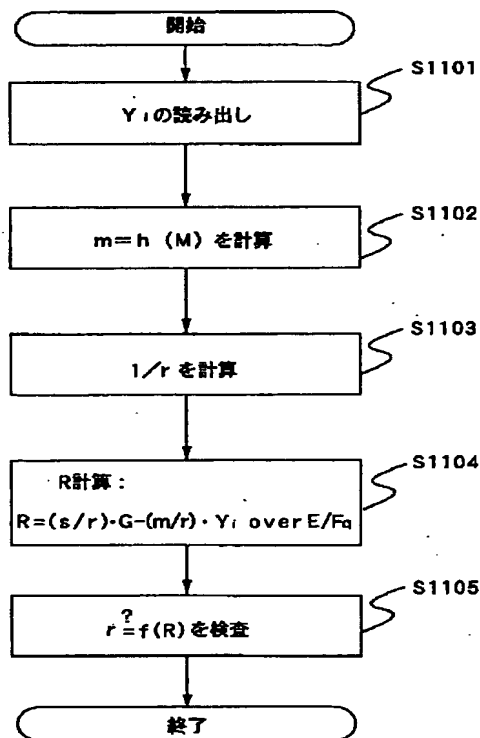
【図 1】



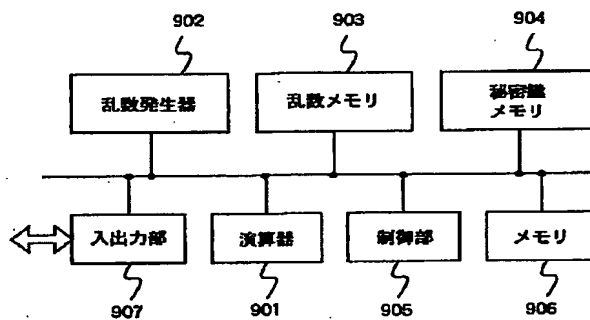
【図 2】



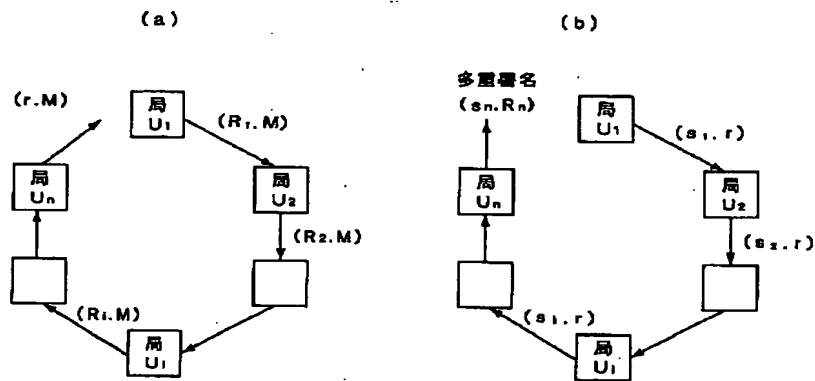
【図 3】



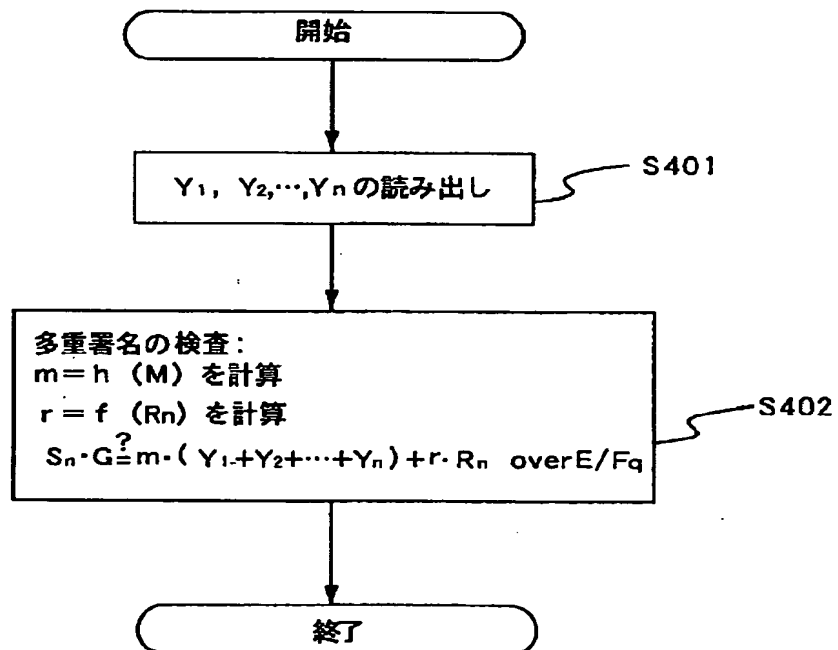
【図 11】



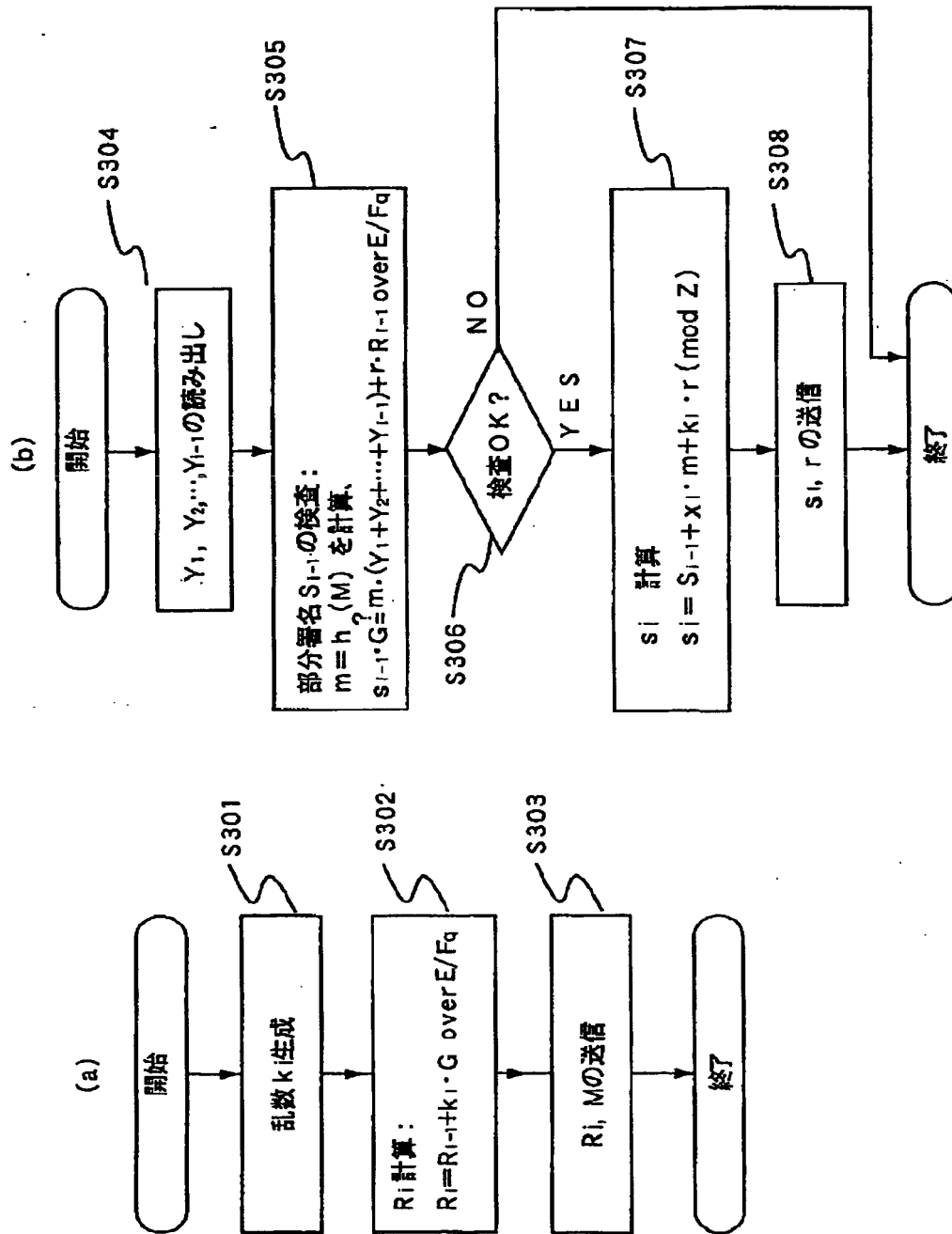
【図4】



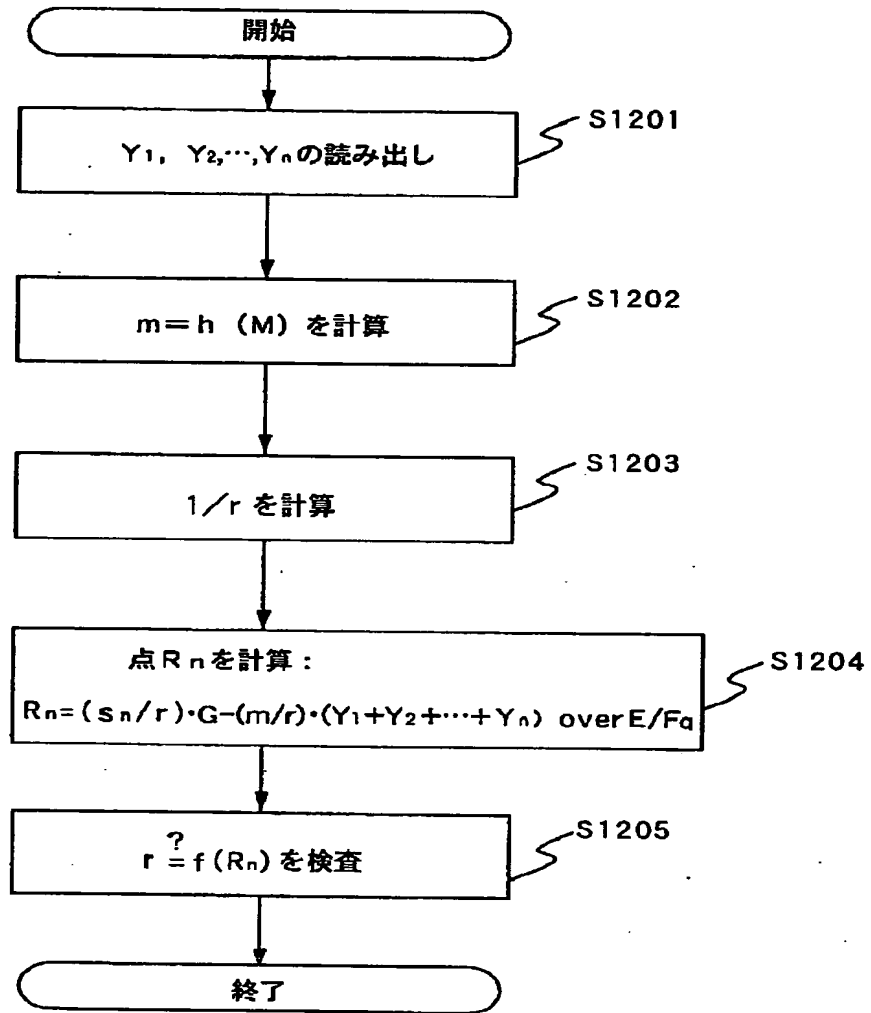
【図6】



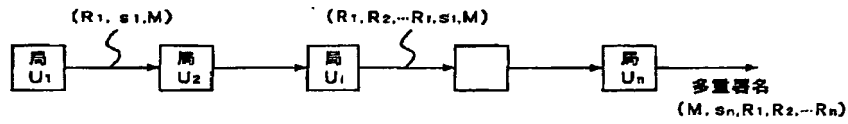
【図5】



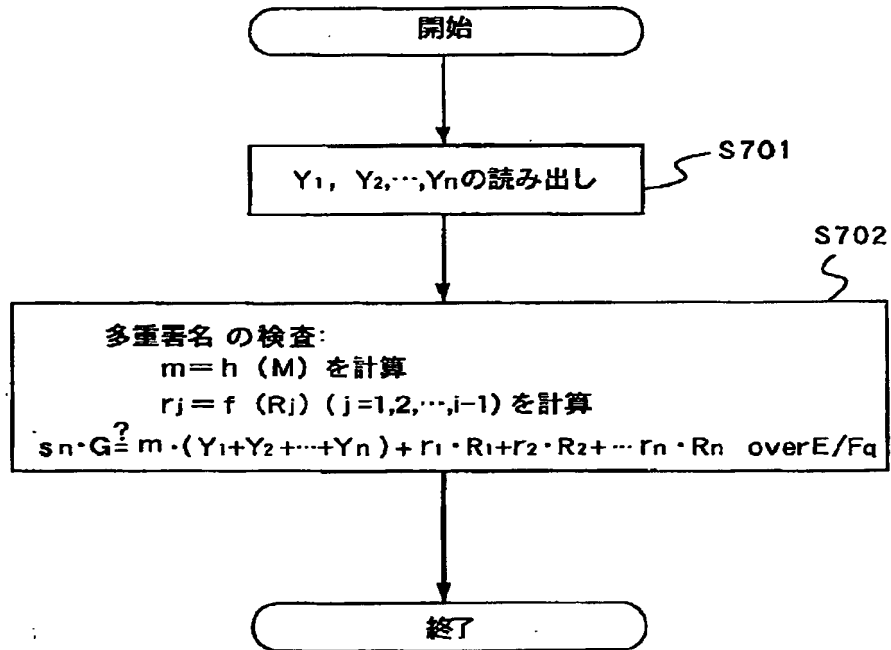
【図7】



【図 8】

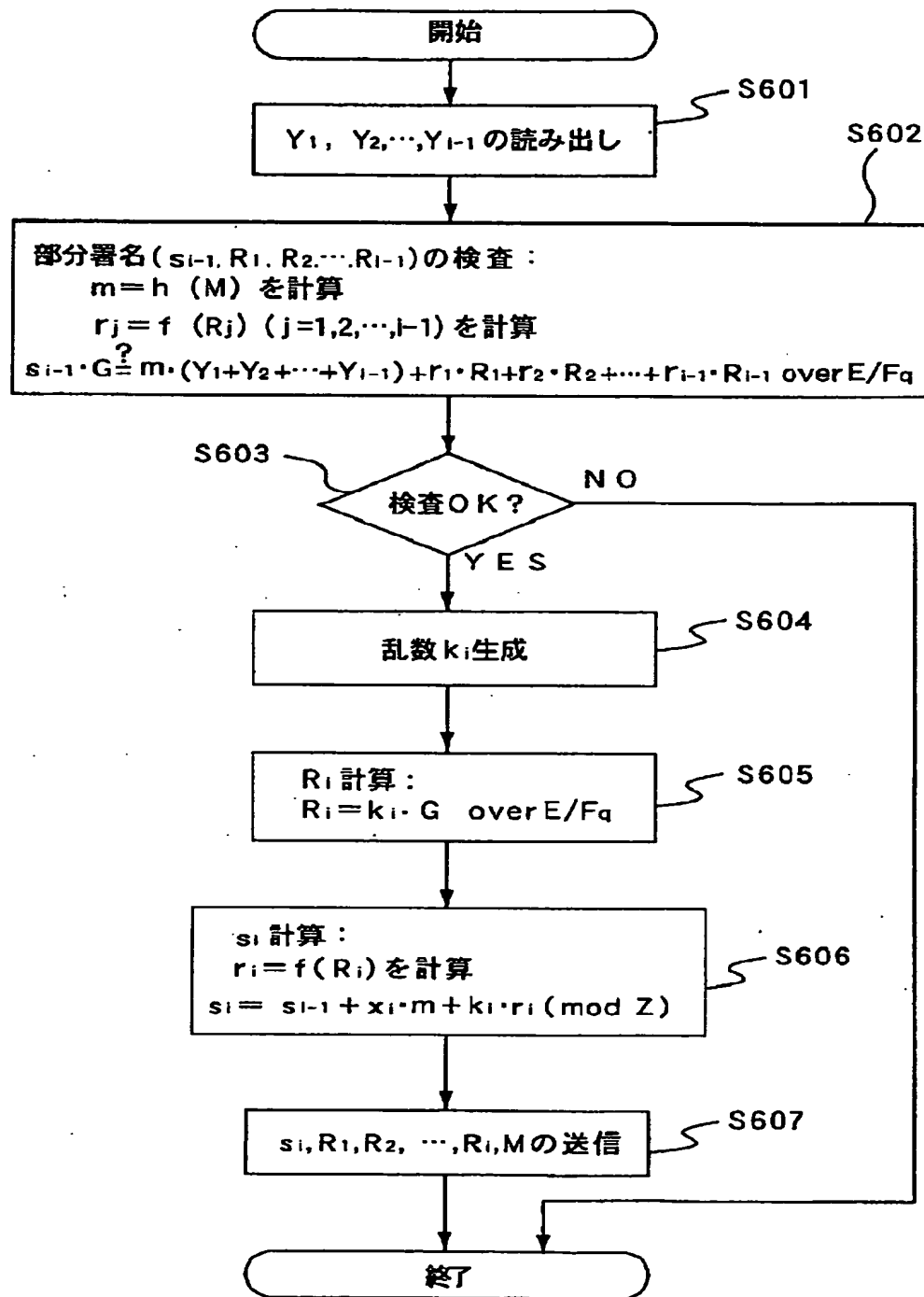


【図 10】

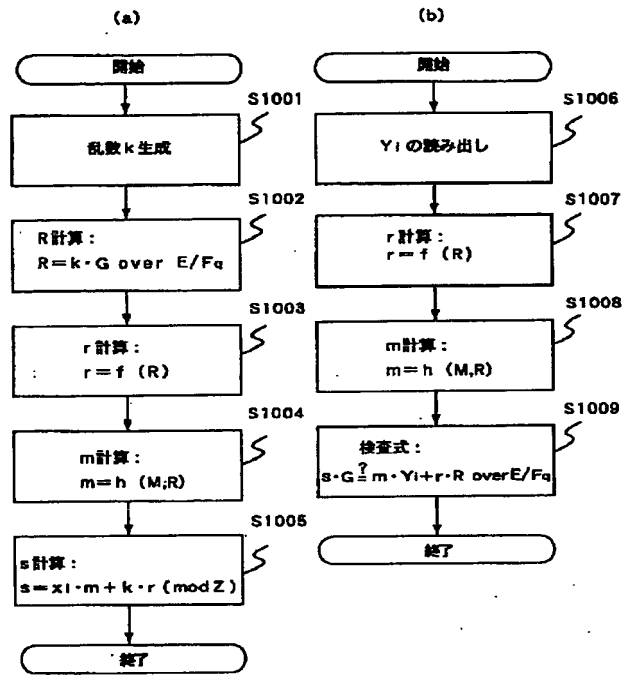




【図9】



【図12】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**